UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 07/23/2004

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	6

DATE MAILED: 07/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/700,656	VATER ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A preliminary amendment was received on 14 February 2001. Claims 1-41 are pending in the present application.

Specification

2. The disclosure is objected to because of the following informalities:

The sections of the specification are not labeled. While the specification does include the required sections of Background, Brief Summary, Brief Description of Drawings, and Detailed Description, each section should be labeled with a section heading. See 37 CFR 1.77 and MPEP § 608.01(a).

Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-25 and 34-41 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-21 are directed to both the data carrier and steps of a method for using the data carrier. Because the claims are directed to both an apparatus and a method, they do not fall into a single statutory class of invention, but rather overlap the two. Therefore, the claims are not statutory. See MPEP § 2173.05(p)II.

Claims 22-25 and 34-41 are directed to methods; however, the claims only state an intended use and do not set forth any steps for performing the method. This results in an improper definition of a method or process, and therefore the claims are not statutory. See MPEP § 2173.05(q).

5. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the statutory classes of invention.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In reference to Claim 1, the claim is directed to a data carrier with intended use as stated. However, the claim does not recite any limitations that clearly describe structures of the apparatus that provide for the stated use. This renders the claim indefinite.

In reference to Claims 3 and 24, the claim recites the limitation "the signal patterns" in line 3 of each claim. The scope of this limitation is unclear. Taking the broadest possible interpretation, if two commands are indistinguishable with respect to the signal patterns that they cause, then any and all outputs of the commands must be identical, and therefore the commands themselves must be equivalent. It is therefore unclear how this further limits the claim, which renders the claim indefinite.

In reference to Claims 5-6 and 26-27, the use of the terms "falsify" and "compensate" are generally unclear. The specification suggests that these terms are intended to mean "encrypt" and "decrypt", respectively, but those terms are also used in the specification in a broader sense. Therefore, the claims are rendered indefinite.

In reference to Claims 9 and 30, the claims recite the limitation "the combination" in line 2 of each claim. It is unclear whether this refers to the combination for compensating of Claims 5 and 26, or to the combination of existing values of Claims 8 and 29, which renders the claims indefinite. For purposes of applying the prior art, it is assumed that this refers to the combination for compensating.

In reference to Claim 13, the claim recites the limitation "it" in line 2 of the claim. It is not clear whether this refers to the operating program or the data carrier itself, which renders the claim indefinite.

In reference to Claims 19 and 40, the claims recite the limitation "it" in line 1 of each claim. It is not clear whether this refers to the data carrier or method, respectively, or to a limitation in a claim from which these claims depend. This renders the claims indefinite.

In reference to Claims 22 and 34, the claims are directed to methods for executing operations in a data carrier; however, there are no method steps recited that clearly describe or disclose the execution of these operations. This renders the claim indefinite.

In reference to Claim 34, the claim recites the limitation "it" in line 2 of the claim. It is not clear whether this refers to the operating system, the data carrier, or the method itself, which renders the claim indefinite.

Claims not explicitly referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-4, 13-25, and 34-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Candelore et al, US Patent 6061449.

In reference to Claim 1, Candelore discloses a data carrier with a semiconductor chip and a memory that is designed to perform security-related operations such that the data being processed cannot be determined from detected signals produced by the chip (column 17, lines 59-67).

In reference to Claims 2-4, Candelore further discloses that commands perform byte-by-byte processing, are indistinguishable with respect to the signal patterns caused by the commands, and lead to a signal pattern that is substantially independent of the data processed (column 23, lines 18-22).

In reference to Claim 13, Candelore further discloses that the order of execution of operations can be varied (column 22, lines 3-14).

In reference to Claim 14, Candelore further discloses that the order of execution is varied at each run (column 23, lines 19-22).

In reference to Claims 15 and 16, Candelore further discloses that the order of execution can be varied according to a fixed principle or randomly (column 23, lines 3-6, where the numbers can be either random or pseudo-random).

In reference to Claim 17, Candelore further discloses that the order of execution can be varied based on the data to be processed (column 14, lines 59-63; column 15, lines 23-25).

In reference to Claims 18 and 19, Candelore further discloses that the order of execution can be fixed before execution of a first operation (column 15, lines 19-21) or before execution of a next operation (column 23, lines 30-34).

In reference to Claim 20, Candelore further discloses that the security-related operations are permutations of data (column 17, lines 61-64).

In reference to Claim 21, Candelore further discloses a smart card (column 18, lines 17-22).

Claims 22-25 and 34-41 are method claims that correspond substantially to Claims 1-4 and 13-20, and are rejected by a similar rationale.

10. Claims 1, 5-12, 21-22, and 26-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnston, US Patent 6373946.

In reference to Claim 1, Johnston discloses a data carrier with a semiconductor chip and a memory that is designed to perform security-related operations such that the

data being processed cannot be determined from detected signals produced by the chip (column 6, lines 20-23).

In reference to Claim 5, Johnston further discloses that the operating program includes combining input data with auxiliary data (column 9, line 66-column 10, line 8) and combining output data with an auxiliary function value (column 10, lines 38-42).

In reference to Claim 6, Johnston further discloses that the combination with the auxiliary function value is done before performing a non-linear operation (column 10, lines 51-53).

In reference to Claim 7, Johnston further discloses that the auxiliary data are varied (column 11, lines 20-23).

In reference to Claims 8-11, Johnston further discloses that new auxiliary values can be generated by combining existing values, that auxiliary data are selected randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (column 9, lines 61-65, where the numbers are pseudo random).

In reference to Claim 12, Johnston further discloses that the combination is an exclusive OR operation (column 9, line 66-column 10, line 12).

In reference to Claim 21, Johnston further discloses a smart card (column 5, lines 59-60).

Claims 22 and 26-33 are method claims that correspond substantially to Claims 1 and 5-12, respectively, and are rejected by a similar rationale.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Matsumura et al, US Patent 4908038, discloses an integrated circuit card that defends against cryptanalytic timing attacks.

b. Fruhauf et al, US Patent 4932053, discloses a circuit to protect chip cards from cryptanalytic attacks depending on analysis of current consumption in the device.

c. Sprunk et al, US Patent 5606616, discloses a cryptographic apparatus that includes combining inputs and outputs of cryptographic functions using XOR operations.

d. Jakobsson, US Patent 6049613, discloses a method and apparatus for protecting data values that includes blinding data before performing cryptographic operations on the data.

e. Moreau, US Patent 6069954, discloses a cryptographic algorithm including combining random values with ciphertext using XOR encryption.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (703) 305-

8902. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (703) 306-3036. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

Matthew B. Smithers

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137